

Melihat URL Yang Sedang Di Akses Dengan Wireshark

Kamaldila Puja Yusnika

kamaldilapujayusnika@gmail.com

http://aldiyusnika.wordpress.com

Lisensi Dokumen:

Copyright © 2003-2013 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

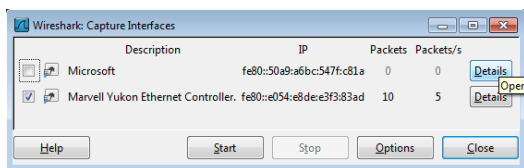
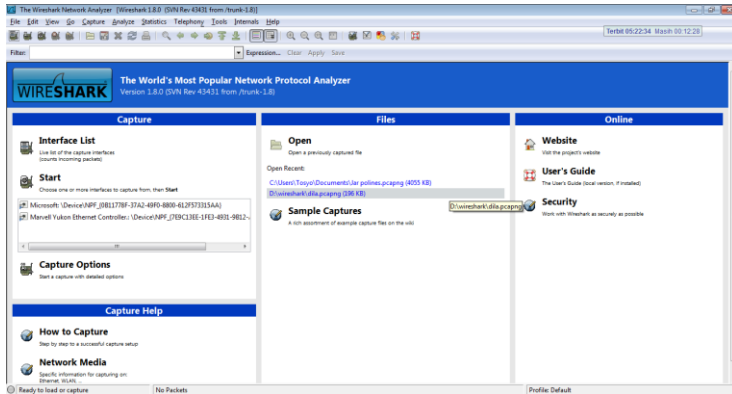
Pendahuluan

Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, dan koneksi ATM.

Dalam sebuah jaringan local, terkadang kita ingin melihat situs apa yang sedang di akses oleh klien pada jaringan tersebut, dengan menggunakan wireshark kita bisa melakukan itu

Dalam kasus ini kita misalkan klien sedang mengakses kaskus.co.id

Pertama buka wireshark dan pilih interface dari computer yang terhubung ke jaringan



Lalu pada sisi klien, melakukan akses ke situs yang di tuju



Lalu scan menggunakan wireshark

No.	Time	Source	Destination	Protocol	Length	Info
952	18.7562940	192.168.1.3	202.169.62.3	HTTP	855	GET /images/2012/09/24/3063581_20120924105814.jpg HTTP/1.1
1036	19.5223540	192.168.1.3	202.169.62.3	HTTP	856	GET /images/2012/09/24/3063581_20120924105814.jpg HTTP/1.1
951	18.7560860	192.168.1.3	202.169.62.3	HTTP	855	GET /images/2012/09/27/3063581_20120927105332.jpg HTTP/1.1
1035	19.5219950	192.168.1.3	202.169.62.3	HTTP	856	GET /images/2012/09/27/3063581_20120927105332.jpg HTTP/1.1
950	18.7553770	192.168.1.3	202.169.62.3	HTTP	853	GET /images/2012/10/01/3063581_20121001031325.gif HTTP/1.1
1031	19.5036770	192.168.1.3	202.169.62.3	HTTP	856	GET /images/2012/10/01/3063581_20121001031325.gif HTTP/1.1
2274	44.0266290	192.168.1.3	159.148.147.201	HTTP	892	GET /images/5/54/Routerboard.png HTTP/1.1
2275	44.0393570	192.168.1.3	159.148.147.201	HTTP	883	GET /images/9/94/Mum.png HTTP/1.1
967	18.8770380	192.168.1.3	50.7.245.26	HTTP	774	GET /images/batik_kaskus-LOGO_seasonal.jpg HTTP/1.1
966	18.8766850	192.168.1.3	50.7.245.26	HTTP	827	GET /images/ba_signuplogin.png HTTP/1.1
1370	26.0160780	192.168.1.3	50.7.245.26	HTTP	827	GET /images/ba_signuplogin.png HTTP/1.1
992	19.0958720	192.168.1.3	50.7.245.26	HTTP	767	GET /images/create-new-thread-2.png HTTP/1.1
1135	21.3853950	192.168.1.3	50.7.245.26	HTTP	764	GET /images/1dfc/self_banner.png HTTP/1.1
2274	44.0263610	192.168.1.3	159.148.147.201	HTTP	905	GET /images/thumb/0/07/News.png/48px-News.png HTTP/1.1
2272	44.0155290	192.168.1.3	159.148.147.201	HTTP	903	GET /images/thumb/1/18/Ros.png/48px-Ros.png HTTP/1.1
2286	44.2352320	192.168.1.3	159.148.147.201	HTTP	909	GET /images/thumb/c/c9/Userman.png/48px-Userman.png HTTP/1.1

Frame 967: 774 bytes on wire (6192 bits), 774 bytes captured (6192 bits) on Interface 0
Ethernet II, Src: Hewlett_77:ba:f2 (00:25:b3:77:ba:f2), Dst: Routerbo_e4:86:c5 (00:0c:42:e4:86:c5)
Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 50.7.245.26 (50.7.245.26)
Transmission Control Protocol, Src Port: 64593 (64593), Dst Port: http (80), Seq: 1, Ack: 1, Len: 720
Hypertext Transfer Protocol
GET /images/batik_kaskus-LOGO_seasonal.jpg HTTP/1.1\r\nHost: img.kaskus.co.id\r\nConnection: keep-alive\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.79 Safari/537.4\r\nAccept: */*\r\nReferer: http://www.kaskus.co.id/\r\nAccept-Encoding: gzip, deflate, sdch\r\nAccept-Language: id-ID, id;q=0.8, en-US;q=0.6, en;q=0.4\r\nAccept-Charset: ISO-8859-1, utf-8;q=0.7, *;q=0.3\r\n

0000 00 0c 42 e4 86 c5 00 25 b3 77 ba f2 08 00 45 00 ..B...% .w...E.
0010 02 f8 67 38 40 00 80 06 00 00 c0 a8 01 03 32 07 ..g8e... ..2.
0020 f5 1a fc 51 00 50 f6 a6 2c a5 4d 39 6f 49 50 18 ...Q.P...Y.OP:
0030 fb 90 eb b7 00 00 47 45 54 20 2f 69 6d 61 67 65GE T /image
0040 73 2f 62 61 74 69 6b 5f 6b 61 73 6b 75 73 2d 4c s/batik_kaskus-L
0050 4e 17 4e 4e 25 61 72 6e 6a 61 6a 3a 63 70 67 0000 0000 0000 0000
File: "C:\Users\Tosyo\AppData\Local\Temp..." Packets: 2433 Displayed: 2433 Marked: 0 Dropped: 0 Profile: Default

Lalu amati pada protokol HTTP, kemudia lihat detailnya di bawah, akan terlihat situs yang sedang di akses, namun untuk protokol HTTPS belum bisa di amati dengan wireshark

Referensi

Percobaan pribadi (aldiyusnika.wordpress.com)

Biografi Penulis



Kamaldila Puja Yusnika. Mahasiswa tingkat akhir Politeknik Negeri Semarang jurusan telekomunikasi, sedang mendalami hal-hal yang behubungan dengan jaringan komputer. Follow my twitter @Aldi_91 atau di blog saya aldiyusnika.wordpress.com